VECTRA SECURITY THAT THINKS® | SWIMLANE

SOLUTION BRIEF

# Automate response and speed remediation with Vectra and Swimlane

## Automated, actionable intelligence to stop threats faster

As the scale and sophistication of network threats continues to increase, businesses need greater visibility into threats and the devices and accounts used in attacks against them. A modern security approach must be built on automated and actionable intelligence to reduce the security operations center (SOC) workload and decrease the time an attacker is allowed to be active in an organization's network.

## Integrate automated threat detection and SOAR

The integration of the Cognito™ automated threat detection and response platform with the Swimlane security orchestration, automation and response (SOAR) platform enables automated threat detection and dramatically reduces SOC workloads.

The Cognito platform is the fastest, most efficient way to find and stop cyberattackers in public clouds, private data centers and enterprise environments. The AI-powered Cognito platform delivers real-time attack visibility and details.

Together, Cognito and Swimlane deliver automated and actionable intelligence that reduces the SOC workload and the time attackers are active inside the network.

## CHALLENGE

Organizations need greater visibility into threats and the devices and accounts used in attacks against them. Security teams are overburdened with alerts, increasing the risk of alert fatigue and allowing attackers to be active inside the enterprise network.

## SOLUTION

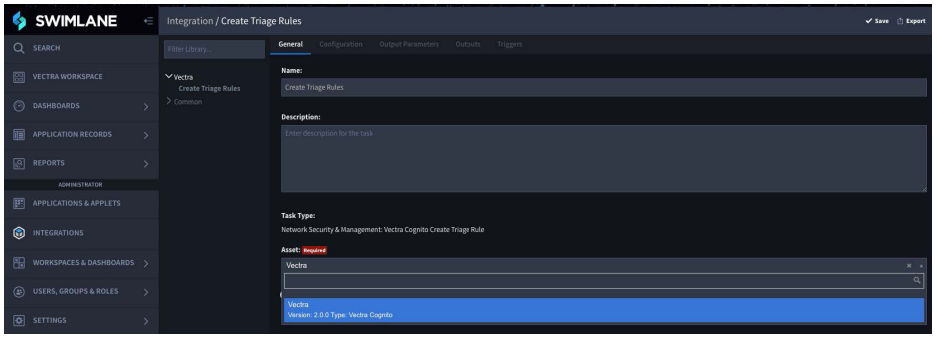
Integration of the Cognito automated threat detection and response platform from Vectra with the Swimlane security orchestration, automation and response (SOAR) platform delivers automated and actionable intelligence that reduces the security team's workload and the time attackers are active inside the network.

## BENEFITS

- Automate network defense by integrating behavior-based threat detection with automated responses
- Trigger different network actions based on type of threat, risk and certainty
- Reduce alert fatigue and free-up security analysts to work on higher value work than triaging the alert backlog

The Cognito platform continuously analyses network traffic to reveal all phases of an active cyberattack, including hidden command and control (C&C) communications, internal reconnaissance, lateral movement, botnet fraud, ransomware and data exfiltration.

The Swimlane SOAR platform eliminates alert backlogs and maximizes the incident response capabilities of overburdened and understaffed SOCs by automating operational workflows and integrating security tools.

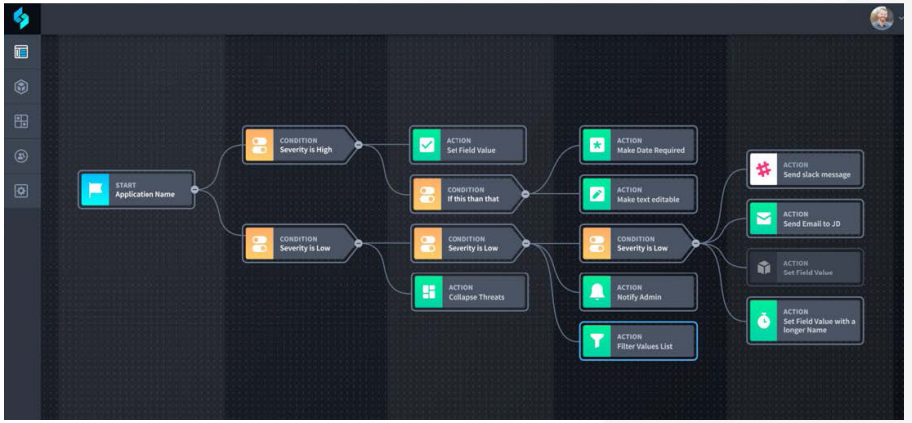



## Automate response workflows

Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito automatically associates all malicious behaviors to the physical network host, even if the IP address changes, and scores the host in terms of its overall risk.

Once the Cognito platform identifies an infected device, its IP address and threat certainty are ingested into Swimlane over an API-first architecture, which centralizes information from the Cognito platform and other systems.

Swimlane then triggers automated response workflows to other security tools to notify users, dynamically segment or quarantine the infected device, stop communication with a C&C server or prevent data exfiltration across all device types and network tiers. Integration between Vectra and Swimlane ultimately reduces the workload of security analysts and the risk of alert fatigue.




## Machine-speed decision making

With this joint solution, Vectra and Swimlane have created a new class of defense, replacing manual incident response processes with machine-speed detection and decision making.

By combining data science and machine learning, Vectra provides inside-the-network threat detection as a next layer of defense in today's security infrastructure.

With sophisticated automation and response tools seamlessly integrated across the security ecosystem, Swimlane enables an instant automated response to quarantine an infected device and stop communication with a C&C server, providing a foundation that secures against the broadest spectrum of threats.

The Cognito platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 34X. Security analysts use the Cognito platform to perform real-time attack hunting by analyzing rich

metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices.

Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint detection and response, network access control (NAC) and firewalls to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

Swimlane is at the forefront of the growing market of security automation, orchestration and response (SOAR) solutions. It delivers scalable and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages.

Swimlane's solution helps organizations address all security operations needs, including prioritizing alerts, orchestrating tools and automating the remediation of threats, protecting against cyberattacks and reducing business risk.

Together, Cognito and Swimlane deliver automated and actionable intelligence that reduces the SOC workload and the time attackers are active inside the network.

## About Vectra

Vectra® is a leader in network detection and response – from cloud and data center apps and workloads to user and IoT devices and accounts. Its Cognito® platform accelerates threat detection and investigation using AI to enrich network metadata and cloud logs it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers four applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. Cognito Detect for Office365 and Azure AD™ finds and stops attacks in enterprise SaaS applications and the Microsoft 365 Ecosystem.

## About Swimlane

Swimlane is a leader in security orchestration, automation and response (SOAR). By automating time-intensive, manual processes and operational workflows and delivering powerful, consolidated analytics, real-time dashboards and reporting from across your security infrastructure, Swimlane maximizes the incident response capabilities of over-burdened and understaffed security operations.

Swimlane was founded to deliver scalable, innovative and flexible security solutions to organizations struggling with alert fatigue, vendor proliferation and chronic staffing shortages. Swimlane is at the forefront of the growing market for security automation and orchestration solutions that automate and organize security processes in repeatable ways to get the most out of available resources and accelerate incident response. Swimlane offers a broad array of features aimed at helping organizations to address both simple and complex security activities, from prioritizing alerts to remediating threats and improving performance across the entire operation. For more information, visit www.swimlane.com.

**For more information please contact a service representative at info@vectra.ai.**

Email info@vectra.ai vectra.ai